Stinks (U)

[redacted]

CT SIGDEV

[redacted]

JUN 2012

Tor Stinks... (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **<u>very small fraction</u>** of Tor users, however, **<u>no</u>** success de-anonymizing a user in response to a TOPI request/on demand.

[redacted]

REMATION II (U)

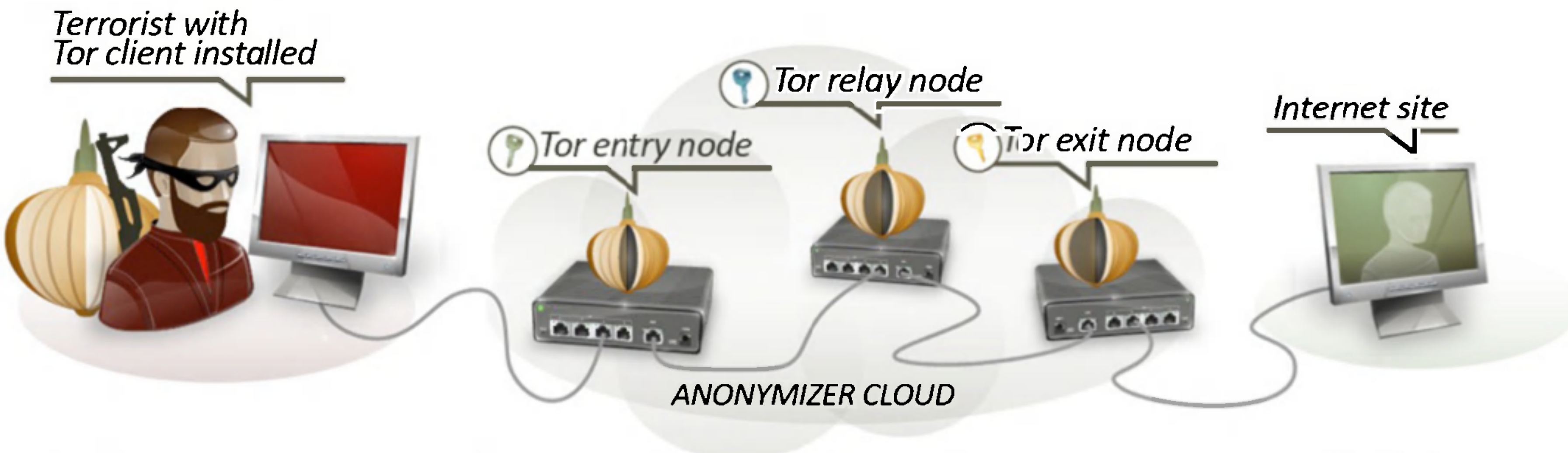
- Joint NSA GCHQ counter-Tor workshop
- Week one at MHS focus on analytics
- Week two at GCHQ focus on exploitation

https://wiki.gchq/index.php?title=REMATION

Laundry List (U)

- Analytics to de-anonymize users
  - Circuit reconstruction (21)
  - Goes inta goes outta/low latency (2)
  - Cookie leakage
  - Dumb users (EPICFAIL)
  - Node Lifespan (17)
  - DNS
- Technical Analysis/Research
  - Hidden services (4, 5, 6, 7)
  - Timing pattern (3)
  - Torservers.net/Amazon AWS
- Exploitation
  - QUANTUM attacks (1, 20, 22)
  - Existing options (8 + 11)
  - Shaping (9 + 16)
  - Web server enabling (10)
  - Nodes (14)
  - Degrade user experience (13 + 18)
- Nodes
  - Baseline our nodes (21)
  - Tor node flooding

Analytics: Circuit Reconstruction (S//SI)



- Current: access to **very** few nodes. Success rate negligible because all three Tor nodes in the circuit have to be in the set of nodes we have access to.
  - Difficult to combine meaningfully with passive SIGINT.
- Goal: expand number of nodes we have access to
  - GCHQ runs Tor nodes under NEWTONS CRADLE (how many?)
  - Other partners?
  - Partial reconstruction (first hops or last hops)?

Analytics: Goes Inta Goes Outta/Low Latency (S//SI)

Find possible alternative accounts for a target: look for connections to Tor, from the target's suspected country, near time of target's activity.

- Current: GCHQ has working version (QUICKANT). R has alpha tested NSA's version. NSA's version produced no obvious candidate selectors.
- Goal: Figure out if QUICKANT works, compare methodologies. Gathering data for additional tests of NSA's version (consistent, random and heavy user)

Analytics: Cookie Leakage (TS//SI)

Use cookies to identify Tor users when they are not using Tor

- Current: preliminary analysis shows that some cookies "survive" Tor use. Depends on how target is using Tor (Torbutton/Tor Browser Bundle clears out cookies).
- Goal: test with cookies **associated** with CT targets
  - Idea: what if we seeded cookies to a target?
  - Investigate Evercookie persistence

Analytics: Cookie Leakage (TS//SI)

- DoubleclickID seen on Tor and non-Tor IPs

[redacted]

Analytics: Dumb Users (EPICFAIL) (S//SI)

GCHQ QFD that looks for Tor users when they are not using Tor.

- Current: GCHQ has working QFD based on hard selector (email, web forum, etc) but does not include cookies.
- Goal: NSA investigating own version (GREAT EXPECTATIONS) that would include cookies.

Analytics: Node Lifespan (S//SI)

How do I know **WHEN** a particular IP was a Tor node as opposed to **IF** it was a Tor node?

- Current: detection done once an hour by NTOC. RONIN stores "last seen" and nodes age off slowly with no accurate lifespan.
- Goal: Working with RONIN to add more details on node lifespan.

Analytics: DNS (TS//SI)

How does Tor handle DNS requests? Are DNS requests going through Tor? Does this depend on how the target is using Tor?

- Current: Still investigating.

Technical Analysis: Hidden Services

(TS//SI)

What do we know about Hidden Services?

- Current: No effort by NSA, some DSD and GCHQ work on ONIONBREATH.
- Goal:
  - Harvest and enumerate .onion URLs
  - Identify similar HS based on referrer fields
  - Distinguish HS from normal Tor clients

Technical Analysis: Timing Pattern

(TS//SI)

Send packets back to the client that are detectable by passive accesses to find client IPs for Tor users.

- Current: GCHQ has research paper and demonstrated capability in the lab.
- Goal: Can we expand to other owned nodes?

Technical Analysis: torservers.net (TS//SI)

Investigate the Amazon AWS cloud instances of Tor servers. How are IPs allocated and reassigned once bandwidth limit is reached? Impact on RONIN's ability to detect nodes?

- Current: GCHQ set up Tor nodes on the AWS cloud during REMATION II.

[redacted]

Exploitation: QUANTUM (TS//SI)

- QUANTUM to degrade/deny/disrupt Tor access?
- QUANTUMCOOKIE – forces clients to divulge stored cookies.

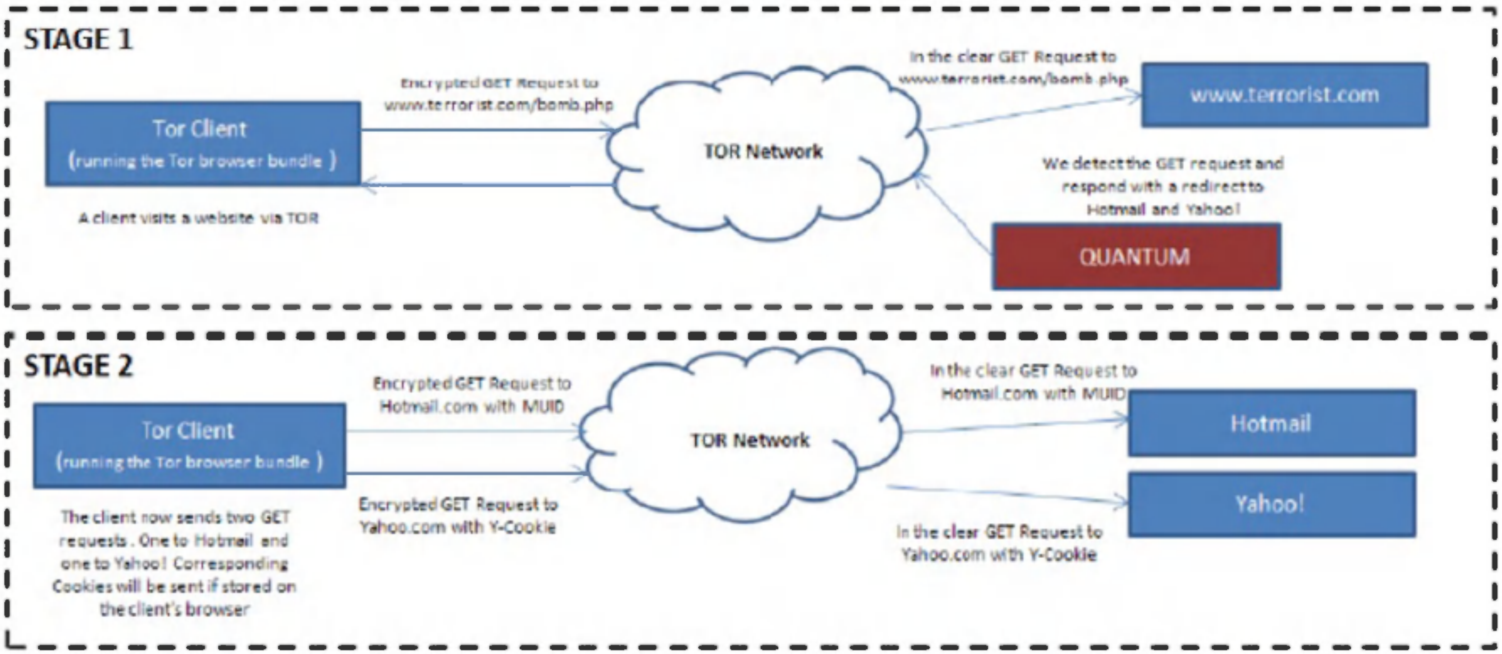


Figure 4: A diagram of how the QUANTUM Survey / Cookie technique works

Exploitation: Existing Options (TS//SI)

Test current CNE techniques (FA and SHORTSHEET) against Torbutton and TBB users.

- Current: Torbutton and TBB prevent CNE success. Possible success against “vanilla” Tor/Vidalia.
- Goal: modifications to initial CNE surveys? Ignore user-agents from Torbutton or TBB? Improve browser fingerprinting? Using javascript instead of Flash?

Exploitation: Shaping (TS//SI)

- Given CNE access to a target computer can we shape their traffic to "friendly" exit nodes?
- Route users to a separate "private" Tor network?
- Stain their traffic or user agent?
- Instruct target computer to use a service that connects outside Tor and reveal true IP?

- Current: Can stain user agent working on shaping.

Exploitation: Web Server Enabling

(TS//SI)

Given CNE access to web server modify the server to enable a “timing/counting” attack similar to timing pattern idea.

- Current: GCHQ has a research paper and demonstrated the technique in the lab.

Exploitation: Nodes (TS//SI)

Can we exploit nodes?

Probably not. Legal and technical challenges.

Exploitation: Degrade Tor experience

(TS//SI)

Given CNE access to a web server make it painful for Tor users?

Given CNE access to a network can we deny/degrade/disrupt Tor users' ?

Nodes: Baseline Our Nodes (TS//SI)

How many nodes do we have cooperative or direct access to? Can we deploy similar code to these nodes to aid with circuit reconstruction?

Can we do packet timing attacks using nodes?

Can we use the nodes to shape traffic flow?

Can we use the nodes to deny/degrade/disrupt comms to certain sites?

Nodes: Tor Node Flooding (TS//SI)

Could we set up a lot of really slow Tor nodes (advertised as high bandwidth) to degrade the overall stability of the network?

Tor Stinks… But it Could be Worse

(S//SI)

- Critical mass of targets use Tor. Scaring them away from Tor might be counterproductive.
- We can **increase** our success rate and provide more client IPs for individual Tor users.
- Will **never get 100%** but we don't need to provide true IPs for every target every time they use Tor.